THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO

WILLIAM FADUIE, ANDREW MUNGER, TOBY CLARKSON GARDNER, and KESTON LEWIS, Plaintiffs, v. **MATCO TOOLS CORPORATION,** Defendant.	Case No.: 5:23-cv-00337 **JUDGE DAVID A. RUIZ** DEMAND FOR JURY TRIAL

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs William Faduie, Andrew Munger, Toby Clarkson Gardner, and Keston Lewis ("Plaintiffs") bring this Class Action Complaint against Matco Tools Corporation ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] of more than 14,000 individuals, including, but not limited to, name, Social Security number, driver's license number, and/or financial account information.

2. According to Defendant's website, "Matco provides mechanics and auto

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

enthusiasts best-in-class service for premium tools, storage, and equipment."[2]

3. Prior to and through March 1, 2022, Defendant obtained the PII of Plaintiffs and Class Members, including by collecting it directly from Plaintiffs and Class Members.

4. Prior to and through March 1, 2022, Defendant stored the PII of Plaintiffs and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

5. On or before December 8, 2022, Defendant learned of a data breach on its network that occurred on or around March 1, 2022 (the "Data Breach").

6. Defendant determined that, during the Data Breach, an unknown actor accessed and/or acquired the PII of Plaintiffs and Class Members.

7. On or around January 26, 2023, Defendant began notifying various states Attorneys General of the Data Breach.

8. On or around January 26, 2023, Defendant began notifying Plaintiffs and Class Members of the Data Breach.

9. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that was accessed and/or acquired by an unauthorized actor included name, Social Security number, driver's license number, and/or financial account information.

10. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive

[2] *See* https://www.matcotools.com/about/ (last visited June 20, 2023).

information.

11. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited over nine months after the Data Breach occurred to report it to the states Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

12. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

13. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

14. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which:

(a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

15. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff William Faduie

16. Plaintiff William Faduie is, and at all times relevant has been, a resident and citizen of Pennsylvania, where he intends to remain. Plaintiff received a Notice Letter from Matco, dated January 26, 2023, on or about that date. The Notice Letter informed Plaintiff that on March 1, 2022, Matco identified unusual activity on its network and that "certain files containing personal information may have been accessed or acquired without authorization[,]" including his full name, address, and Social Security number. The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

Plaintiff Andrew Munger

17. Plaintiff Andrew Munger is, and at all times relevant has been, a resident and citizen of Florida, where he intends to remain. Plaintiff received a Notice Letter from Matco, dated January 26, 2023, on or about that date. The Notice Letter informed Plaintiff that on March 1, 2022, Matco identified unusual activity on its network and that "certain files containing personal information may have been accessed or acquired without authorization[,]" including his full name, address, and Social Security number. The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

Plaintiff Toby Clarkson Gardner

18. Plaintiff Toby Clarkson Gardner is, and at all times relevant has been, a resident and citizen of Wyoming, where he intends to remain. Plaintiff received a Notice Letter from Matco, dated January 26, 2023, on or about that date. The Notice Letter informed Plaintiff that on March 1, 2022, Matco identified unusual activity on its network and that "certain files containing personal information may have been accessed or acquired without authorization[,]" including his full name, address, and Social Security number. The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

Plaintiff Keston Lewis

19. Plaintiff Keston Lewis is, and at all times relevant has been, a resident and citizen of Georgia, where he intends to remain. Plaintiff received a Notice Letter from Matco, dated January 26, 2023, on or about that date. The Notice Letter informed Plaintiff that on March 1, 2022, Matco identified unusual activity on its network and that "certain files containing personal information may have been accessed or acquired without authorization[,]" including his full name,

address, and Social Security number. The letter further advised that Plaintiff that he could participate in credit monitoring services detecting suspicious activity.

20. Defendant obtained and continues to maintain Plaintiffs' and Class Members' PII and has a continuing legal duty and obligation to protect that sensitive information from unauthorized access and disclosure. Defendant required the PII from Plaintiffs. Plaintiffs, however, would not have entrusted their PII to Defendant had they known that it would fail to maintain adequate data security. Plaintiffs' PII was compromised and disclosed as a result of the Data Breach.

Defendant Matco

21. Defendant Matco is a corporation engaged in the manufacture and sale of tools for resale by distributors and franchisees. Matco is a Delaware corporation with a principal place of business at 4403 Allen Road, Stow, Ohio.

22. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

23. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

24. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the

proposed class, and at least one Class Member, including each of the Plaintiffs, is a citizen of a state different from Defendant to establish minimal diversity.

25. Defendant is a citizen of Ohio because its principal place of business in Stow, Ohio.

26. The Northern District of Ohio has personal jurisdiction over Defendant because it conducts substantial business in Ohio and this District and collected and/or stored the PII of Plaintiffs and Class Members in this District.

27. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

28. Defendant manufactures, sells, and services more than thousands of professional tools for various purposes.[3]

29. Matco started operations in 1946. Since 1979, Matco had sold its automotive tools and produce to professional mechanics, enthusiasts, and those who value automotive tools through a network of independent franchised mobile tool distributors. [4]

30. Matco distributors operate in all 50 states, Canada, and Puerto Rico.

31. Plaintiffs and Class Members were customers and/or employees of Defendant whose PII was required to be provided, and was in fact provided, to Defendant in conjunction with manufacturing of car components or during the course of their employment with Defendant. Plaintiffs' and Class Members' PII were required to fill out various forms, including without

[3] https://www.matcotools.com/about/ (last visited June 20, 2023).
[4] *Id*.

limitation employment paperwork and applications, tax documents, various authorizations, other form documents associated with the manufacturing of car components, and employment documentation.

32. Plaintiffs and Class Members relied on the sophistication of Defendant and its network to keep their PII confidential and securely maintained, to use this information for business and/or employment purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

33. Defendant required the submission of and voluntarily accepted the PII as part of its business and had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Matco has a legal duty to keep employee and consumer PII safe and confidential.

34. The information held by Defendant in its computer systems and networks included the PII of Plaintiffs and Class Members.

35. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII.

36. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Matco assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

37. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

38. Defendant collected the PII of Plaintiffs and Class Members and stored it, unencrypted, on Defendant's internet-accessible network.

39. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs

and Class Members from involuntary disclosure to third parties.

The Data Breach

40. On or about January 26, 2023, Defendant sent Plaintiffs and Class Members a *Notice of Data Security Incident* (the "Notice Letter") and submitted sample notices to various states' Attorneys General. Defendant informed Plaintiffs and other Class Members that:

> Matco Tools ("Matco") is committed to protecting the privacy and security of the information we maintain. We are writing to inform you about a data security incident that may have involved some of your information.
>
> This notice explains the incident, measures we have taken, and some steps you can take in response. Matco recently concluded its investigation of an incident that involved suspicious activity where a server was copying data outside of the network. Upon first suspecting unauthorized access, we immediately disconnected the systems involved from the broader network, disabled the accounts associated with that activity, and launched an investigation.
>
> The investigation determined that an unauthorized party gained access to the network on March 1, 2022. Matco then used the investigation's findings to determine which files and folders might have been subject to unauthorized access and conducted a thorough review of the data involved. On December 8, 2022, we determined that a file or folder was accessed by the unauthorized actor which contained your name and <<Variable Data 1>>.[5]

41. The Notice Letter Defendant sent to Plaintiffs stated that Plaintiffs' name and Social Security number were accessed during the Data Breach.

42. Defendant reported to the Attorney General of Maine that name, Social Security number, driver's license number, bank account number, and date of birth were impacted in the Data Breach.[6]

---

[5]https://apps.web.maine.gov/online/aeviewer/ME/40/e070fe84-fe8b-4442-a77e-e4c0635552e1.shtml (data breach notice letter include via hyperlink under "Copy of notice to affected Maine residents").

[6] *Id.* at 1.

43. Defendant admitted in the Notice Letter and the sample notices and reports it sent to the states' Attorneys General that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members, including name, Social Security number, driver's license number, and/or financial account information.

44. In response to the Data Breach, Defendant claims that it "has implemented additional security measures to enhance the security of its environment, is supporting the conversion of its partners to more modern systems, and continuing to train its employees concerning data security."[7]

45. To date, Matco has not revealed when the unauthorized actor first gained access to a portion of Defendant's network, nor has it revealed the mechanism by which the unauthorized actor first gained access to Defendant's network.

46. Upon information and belief, the unauthorized actor gained access to Matco's network well in advance of the December 8, 2022, date that the intrusion was first discovered by Matco, meaning that the unauthorized actor had unfettered and undetected access to Defendant's networks for a considerable period of time prior to Matco becoming aware of the unauthorized access to its computer systems and network.

47. However, upon information and belief, Matco has no methods, policies, or procedures in place that would afford its employees and customers (like Plaintiffs and Class Members) any mechanism or opportunity to report misuse of the data back to Matco, and the investigation commissioned by Matco did not survey Matco's clients whose data was breached for evidence of misuse.

48. The attacker accessed, and likely acquired, files on the server containing PII,

[7] *Id.*

including names and Social Security numbers.

49. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

50. Plaintiffs further believe their PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

51. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

52. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

53. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

54. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

55. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

56. Given that Defendant was storing the PII of Plaintiffs and Class Members,

Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

57. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers and employees, including Plaintiffs and Class Members.

58. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[8]

59. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "*[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies*. They breach networks, use specialized tools to maximize damage, *leak corporate information on dark web portals*, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[9]

60. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that *"[m]alicious actors have adjusted their ransomware tactics to be more destructive and impactful and have also exfiltrated victim*

[8] FBI, *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations* (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited June 15, 2023).

[9] ZDNet, *Ransomware mentioned in 1,000+ SEC filings over the past year* (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited June 15, 2023).

data and pressured victims to pay by threatening to release the stolen data." [10]

61. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

62. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

63. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

64. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members.

65. Defendant acquired, collected, and stored the PII of Plaintiffs and the Class.

66. As part of being a customer and/or employee of Defendant, Plaintiffs and Class Members, are required to give their sensitive and confidential PII to Defendant. Defendant retains

[10] U.S. CISA, Ransomware Guide, *available at* https://www.cisa.gov/stopransomware/ransomware-guide (last visited June 15, 2023).

and stores this information, and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to sell or manufacture automobile parts or employ anyone for the purpose of assisting Defendant with manufacturing car components.

67. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

68. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

69. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[11]

70. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from

[11] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited June 15, 2023).

reaching end users.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

71. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are

[12] *Id.* at 3-4.

the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[13]

72. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

[13] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited June 15, 2023).

- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

73. Given that Defendant was storing the PII of more than 14,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

74. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data

[14] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited June 15, 2023).

Breach and the exposure of the PII of more than 14,000 individuals, including Plaintiffs and Class Members.

Securing PII and Preventing Breaches

75. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

76. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

77. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

78. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[16]

79. Defendant knew and understood unprotected or exposed PII in the custody of manufacturing companies, such as Defendant, is valuable and highly sought after by nefarious

[15] 17 C.F.R. § 248.201 (2013).
[16] *Id.*

third parties seeking to illegally monetize that PII through unauthorized access, as these companies maintain highly sensitive PII of employees and consumers, including Social Security numbers and financial information.

80. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

81. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[19]

82. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

83. Social Security numbers, for example, are among the worst kind of PII to have

[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed June 15, 2023).
[18] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed June 15, 2023).
[19] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed June 15, 2023).

stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[20]

84. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

85. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

86. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to

---

[20] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited June 15, 2023).

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited June 15, 2023).

change—one's Social Security number.

87. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[22]

88. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

89. The fraudulent activity resulting from the Data Breach may not come to light for years.

90. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

91. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on

[22] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed June 15, 2023).

[23] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed June 15, 2023).

Plaintiffs and Class Members as a result of a breach.

92. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

93. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's contract search tool, amounting to potentially tens of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

94. To date, Defendant has offered Plaintiffs and Class Members only one year of complimentary identity monitoring services through IDX. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

95. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

96. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendant Violated the FTC Act

97. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this

regard.

98. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

Plaintiff William Faduie's Experience

99. Plaintiff Faduie was required to provide and did provide his PII to Defendant during the course of his employment with Defendant. The PII included his name and Social Security Number.

100. To date, Matco has done next to nothing to adequately protect Plaintiff Faduie and Class Members, or to compensate them for their injuries sustained in this Data Breach.

101. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff Faduie and Class Members by requiring them to expend time signing up for the service and addressing timely issues.

102. Plaintiff Faduie and Class Members have been further damaged by the compromise of their PII.

103. Plaintiff Faduie's PII was compromised in the Data Breach, and was likely stolen and in the hands of cybercriminals who illegally accessed Matco's network for the specific purpose of targeting the PII.

104. Plaintiff Faduie typically takes measures to protect his PII, and is very careful about

sharing his PII. Faduie has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

105. Plaintiff Faduie stores any documents containing his PII in a safe and secure location, and he diligently chooses unique usernames and passwords for his online accounts.

106. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

107. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of obtaining employment from Defendant, which was compromised in and as a result of the Data Breach.

108. Plaintiff Faduie suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

109. Plaintiff Faduie has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security Number, being placed in the hands of criminals.

110. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from Plaintiff when he began employment with Defendant. Plaintiff, however, would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff Faduie's PII was compromised and disclosed as a result of the Data Breach.

111. As a result of the Data Breach, Plaintiff Faduie anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Andrew Munger's Experience

112. Plaintiff Munger purchased tools from Defendant, using credit, prior to the Data Breach and received Defendant's *Notice of Data Security Incident*, dated January 26, 2023, on or about that date. The notice stated that Plaintiff's personal information, including name and Social Security number, were accessed by an unauthorized actor.

113. As a result of the Data Breach, Plaintiff Munger's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Munger's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Munger will have to worry about when and how his sensitive information may be shared or used to his detriment.

114. After the Data Breach, Plaintiff Munger was notified that an unknown individual using Plaintiff's identity applied for an automobile loan with Ally Financial in May 2022, approximately two months after the Data Breach occurred.

115. As a result of the Data Breach notice, Plaintiff Munger spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Security Incident* and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

116. Additionally, Plaintiff Munger is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

117. Plaintiff Munger stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

118. Plaintiff Munger suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

119. Plaintiff Munger has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals.

120. Plaintiff Munger has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Toby Clarkson Gardner's Experience

121. Plaintiff Munger had previously applied to work for Matco in 2015, prior to the Data Breach, and received Defendant's *Notice of Data Security Incident*, dated January 26, 2023, on or about that date. The notice stated that Plaintiff's personal information, including name and Social Security number, were accessed by an unauthorized actor.

122. As a result of the Data Breach, Plaintiff Clarkson Gardner's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Clarkson Gardner's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Clarkson Gardner will have to worry about when and how his sensitive information may be shared or used to his detriment.

123. After the Data Breach, Plaintiff Clarkson Gardner was notified that he was the victim of identity theft, as some unidentified individual residing in California attempted to make a

purchase using his bank account following the breach.

124. In fact, in approximately March 2022, Plaintiff Clarkson Gardner received a telephone call from Points West Community Bank regarding the fraudulent transactions he did not authorize.

125. As a result of the Data Breach notice, Plaintiff Clarkson Gardner spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Security Incident* and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

126. Additionally, Plaintiff Clarkson Gardner is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

127. Plaintiff Clarkson Gardner stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

128. Plaintiff Clarkson Gardner suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

129. Plaintiff Clarkson Gardner has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals.

130. Plaintiff Clarkson Gardner has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Keston Lewis's Experience

131. Plaintiff Lewis purchased tools from Defendant, using credit, prior to the Data Breach and received Defendant's *Notice of Data Security Incident*, dated January 26, 2023, on or about that date. The notice stated that Plaintiff's personal information, including name and Social Security number, were accessed by an unauthorized actor.

132. As a result of the Data Breach, Plaintiff Lewis's sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Lewis's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Lewis will have to worry about when and how his sensitive information may be shared or used to his detriment.

133. As a result of the Data Breach notice, Plaintiff Lewis spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Security Incident* and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

134. Additionally, Plaintiff Lewis is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

135. Plaintiff Lewis stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

136. Plaintiff Lewis suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

137. Plaintiff Lewis has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially

his Social Security number, being placed in the hands of criminals.

138. Plaintiff Lewis has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

139. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

140. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All persons Matco Tools identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach or around January 26, 2023 (the "Nationwide Class").**

141. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

> **All individuals who made purchases from Defendant on or before March 1, 2022, and whose PII was accessed and/or acquired in the data incident that is the subject of the Notice of Data Security Incident that Defendant sent to Plaintiffs and Class Members on or around January 26, 2023 (the "Customers Subclass") (collectively, with the Nationwide Class, "the Classes").**

142. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

143. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

144. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant reported to the Maine attorney general that 14,342 individuals were impacted in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

145. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures

and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

146. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

147. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

148. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent

and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

149. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

150. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that

experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

151. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

152. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

153. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

154. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

155. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

156. Plaintiffs and the Nationwide Class incorporate by reference all other allegations in the Complaint as if fully set forth herein.

157. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

158. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

159. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

160. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

161. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

162. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Defendant acquired Plaintiffs' and the Nationwide Class's confidential PII in the course of its business practices.

163. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

164. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

165. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

166. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

167. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and likely remains in, Defendant's possession.

168. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

169. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

170. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

171. Defendant has admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

172. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

173. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

174. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

175. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

176. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain in an Internet-accessible environment.

177. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

178. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and

the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

179. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

180. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

181. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

182. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

183. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

184. In failing to secure Plaintiffs' and Class Members' PII and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiffs, therefore, in addition to seeking actual damages, seek punitive damages on behalf of themselves and the Class.

185. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to patient information.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

186. Plaintiffs and the Customer Subclass by reference all other allegations in the Complaint as if fully set forth herein.

187. In making purchases from Defendant, Plaintiffs and the Customer Subclass provided and entrusted their PII to Defendant.

188. Defendant required Plaintiffs and the Customer Subclass to provide and entrust their PII as condition of making purchases from Defendant.

189. As a condition of making purchases from Defendant, Plaintiffs and the Customer Subclass provided and entrusted their PII. In so doing, Plaintiffs and the Customer Subclass entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and the Customer Subclass if their PII had been compromised or stolen.

190. Plaintiffs and the Customer Subclass fully performed their obligations under the implied contracts with Defendant.

191. Defendant breached the implied contracts it made with Plaintiffs and the Customer Subclass by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

192. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Customer Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity

theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

193. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Customer Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Customer Subclass)

194. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth herein.

195. This claim is plead in the alternative to any claim for breach of contractual obligations.

196. Defendant benefited from receiving Plaintiffs' and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

197. Defendant also understood and appreciated that Plaintiffs' and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

198. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of purchasing services from Defendant, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiffs and Class members should have received adequate protection and data security for such PII held by Defendant.

199. Defendant knew Plaintiffs and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

200. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiffs and Class Members.

201. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

202. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

203. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

204. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT IV
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class)

205. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth herein.

206. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

207. The Ohio Consumer Sales Practices Act ("CSPA") similarly prohibits "unfair or deceptive act[s] or practice[s] in connection with a consumer transaction." R.C. 1345.02(A). Moreover, the CSPA requires courts to "give due consideration and great weight to federal trade commission orders, trade regulation rules and guides, and the federal courts' interpretations of subsection 45 (a)(1) of the 'Federal Trade Commission Act,' 38 Stat. 717 (1914), 15 U.S.C.A. 41, as amended." R.C. 1345.02(C).

208. Defendant violated the CSPA and Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

209. Defendant's violations of the FTC Act and CSPA constitute negligence per se.

210. The harm that has occurred is the type of harm the FTC Act and CSPA were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

211. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach

reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

212. Plaintiffs and the Class repeat and re-allege each and every allegation contained in the Complaint as if fully set forth herein.

213. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

214. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

215. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Nationwide Class's PII, including Social Security numbers, while storing it in

an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security number of Plaintiffs.

216. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiffs and the Nationwide Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

217. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards;

d. implement an education and training program for appropriate employees regarding cybersecurity.

218. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

219. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

220. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Customer Subclass and appointing Plaintiffs and their Counsel to represent such Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and

internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as

necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: June 20, 2023

Respectfully Submitted,

/s/ Terence R. Coates

Terence R. Coates (0085579)
Dylan J. Gould (0097954)
Jonathan T. Deters (0093976)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Tel: 513.651-3700
tcoates@msdlegal.com
dgould@msdlegal.com
jdeters@msdlegal.com

David K. Lietz (*pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20115
Phone: (866) 252-0878
dlietz@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

Jesse A. Shore (0091730)
Morgan & Morgan, Kentucky PLLC
300 Madison Avenue, Suite 200
Covington, KY 41011
Telephone: (859) 899-8786
Facsimile: (859) 899-8807
jshore@forthepeople.com

Ryan D. Maxey (*pro hac vice*)
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
rmaxey@ForThePeople.com

Matthew R. Wilson (Bar No. 0072925)
Michael J. Boyle, Jr. (Bar No. 0091162)
Jared W. Connors (Bar No. 0101451)
MEYER WILSON CO., LPA
305 W. Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066
mwilson@meyerwilson.com
mboyle@meyerwilson.com
jconnors@meyerwilson.com

Samuel J. Strauss*
Raina Borrelli*
TURKE & STRAUSS LLP
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice application forthcoming*